基于SM9的环签名：常数级计算开销的方案构造

谢振杰[1,2]，刘胜利[1]，贾志鹏[1]，翟锦源[1]，刘成[1]
（1.信息工程大学网络空间安全教育部重点实验室，河南 郑州 450001；2.中国人民解放军78156部队，重庆 400039）

摘　要：针对现有标识环签名方案的性能瓶颈，提出一种基于国密算法SM9的高效环签名方案。通过优化群运算结构，将签名与验证的计算开销从线性级降至常数级，显著提升了标识环签名的计算性能。现有标识环签名方案需对环成员逐项执行双线性对或标量乘等耗时运算，而所提方案将环成员信息转移至轻量的有限域运算，使耗时运算次数与环规模无关。在随机预言机模型下，证明了所提方案满足不可伪造性和完全匿名性。实验表明，当环成员数量为1 024时，所提方案的签名和验证耗时分别为37.06 ms和48.59 ms，较现有最优方案提升241.61倍和10.11倍，即使计入线性的通信开销，其综合效率仍有明显优势。

关键词：环签名；SM9算法；基于标识的密码；常数级开销；国密算法
中图分类号：TP309.7
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025217

SM9-based ring signature: a scheme with constant-time computational overhead

XIE Zhenjie[1,2], LIU Shengli[1], JIA Zhipeng[1], ZHAI Jinyuan[1], LIU Cheng[1]
1. Key Laboratory of Cyberspace Security, Ministry of Education, Information Engineering University, Zhengzhou 450001, China
2. Unit 78156 of the Chinese People's Liberation Army, Chongqing 400039, China

Abstract: To address the performance bottleneck of existing identity-based ring signature schemes, an efficient scheme based on the Chinese national cryptographic standard SM9 was proposed. By optimizing the group operation structure, the computational overhead of signing and verification was reduced from linear to constant time, leading to a substantial improvement in performance. In contrast to existing schemes requiring computationally intensive operations (e.g., bilinear pairings or scalar multiplications) per ring member, the proposed scheme shifted member-related calculations to lightweight finite field operations, thus maintaining a fixed count of computationally intensive operations regardless of ring size. Under the random oracle model, the scheme was demonstrated to achieve existential unforgeability and full anonymity. Experimental evaluations indicate that for a ring size of 1 024, signing and verification times are 37.06 ms and 48.59 ms respectively, representing performance gains of 241.61× and 10.11× over current state-of-the-art alternatives. The overall efficiency retains a significant advantage even when considering linear communication overhead.

Keywords: ring signature, SM9 algorithm, identity-based cryptography, constant-time overhead, domestic cryptographic algorithm

收稿日期：2025–09–13；**修回日期：**2025–11–12
通信作者：刘胜利，mr_shengliliu@163.com
基金项目：装备预先研究基金资助项目（No.30603010601）
Foundation Item：Equipment Pre Research Project (No.30603010601)

0　引言

环签名作为一种特殊的数字签名方案，由Rivest等[1]于2001年首次提出，其核心思想是允许签名者代表一个潜在签名群体（称为环）对消息进行签名，同时保持签名者在环中的匿名性。相较于群签名，环签名不需要设置群管理员，成员间地位平等且不需要协作。尽管早期方案因签名数据呈环状结构而得名，但后续研究表明，只要满足自发性和匿名性要求，即使非环状结构也可归类为环签名[2]。环签名凭借其不可伪造性和匿名性，在区块链[2]、电子投票[3]、数字货币[4]及多方计算[5]等隐私敏感领域展现出重要应用价值。自该概念提出以来，研究者已基于不同密码学原语开发了多种环签名方案，包括RSA[1]、离散对数[6]、双线性对[7]和格理论[8]等实现方式。

传统环签名方案依赖公钥基础设施（PKI, public key infrastructure），但PKI体系存在证书管理复杂、验证效率低下等问题，尤其在环规模较大时，频繁的证书请求易导致系统性能瓶颈。基于标识的密码体制（IBC, identity-based cryptography）通过将用户身份直接作为公钥，规避了PKI的证书管理难题，提升了系统效率。我国自主设计的国密算法SM9是一种基于椭圆曲线双线性对的IBC，其涵盖数字签名、密钥交换、密钥封装和加密[9-10]。相较于RSA等传统公钥密码，SM9在相同安全强度下具有更短的密钥长度和更高的计算效率，同时避免了PKI的运维负担。近年来，基于SM9的IBC应用方案研究已取得显著进展，包括环签名[11-14]、可搜索加密[15]、属性签名[16]、代理重加密[17]及容错加密[18]等。

本文在SM9数字签名算法的基础上，设计了一种标识环签名（IBRS, identity-based ring signature）方案，主要贡献在于将签名与验证过程中原本与环规模线性相关的耗时运算全部压缩至常数级，实现了计算性能的突破。在随机预言机（RO, random oracle）模型下，严格证明了方案满足不可伪造性和完全匿名性的安全要求。理论分析与实验表明，所提方案的签名与验证效率显著优于现有同类方案，在环规模较大时有数量级上的提升。由于目前尚无可靠方法在动态环时实现严格常数级计算开销，本文中的“常数级计算开销”指所有耗时运算的次数均为常数，其在常见的环规模下具有近似常数级的性能表现。

1　相关工作

Zhang等[7]开创了IBRS研究，后续工作多沿用双线性对技术[19-21]。Brakerski等[22]建立了将数字签名转化为环签名的一般框架，但其计算和通信开销均与环成员数量n成线性关系，效率瓶颈明显。为突破这一限制，Dodis等[23]首次基于累加器实现了常数级环签名长度，且验证时间与环规模无关。Nguyen[24]和Hu等[25]进一步结合累加器与双线性对，构建了具有常数级环签名长度的IBRS方案。

近年来，国密算法与环签名的融合研究从参考成熟的国际密码方案逐渐向算法自主设计转变，取得了一系列成果。彭聪等[11]首次将SM9算法引入环签名设计，较此前基于国际标识密码的同类方案压缩了环签名长度，但计算和通信开销都与n线性相关。邓浩明等[26]提出了基于SM9的门限环签名方案，因验证阶段的双线性对次数与门限值线性相关，计算效率受限。饶金涛等[3]描述了基于SM9的盲签名和环签名方案，并应用于电子投票，因其验证算法未纳入签名者私钥要素，存在重放攻击风险。安浩杨等[13]首次基于SM9提出了常数级环签名长度的方案，但累加器的引入使公共参数与最大环成员数线性相关，此外，该方案的设计思路和计算过程比较复杂，安全性证明不够充分，仅在环较大（$n > 20$）时签名长度才小于文献[11]方案。谢振杰等[12]在文献[11]基础上提出的方案将最耗时的双线性对等效替换后，计算效率提升超过1倍，签名长度减小近一半。谢振杰等[14]采用累加器实现了常数级环签名长度的SM9可追踪环签名方案，强化了安全性证明工作，计算过程较文献[13]方案大幅简化，计算效率有所提升，签名长度减小近80%。然而，文献[13-14]均假定由累加器的构造者向用户直接提供累加器以实现常数级计算开销，但该假设要求构造者提前获知环成员和签名者信息并保持在线，局限性较大。若由用户自行计算累加器，则文献[13-14]的计算开销都与n线性相关，面对更大的环规模（如$n > 1\ 000$）时仍会产生高延迟。上述基于SM9设计的IBRS方案既涵盖国外经典文献的成熟模式，又包含国内自主设计的创新算法，总体性能不亚于基于国际密码算法的同类方案。

国内外密码学者通过引入新的设计范式，逐步实现了对数级或常数级的环签名时空开销。Bootle

等[27]指出，目前高效的环签名方案通常需要依赖于一个维护主密钥的信任机构，或者采用基于累加器的方法。通过引入优化的预处理参数，其构建了首个签名大小和验证时间均为对数级的可链接环签名（LRS, linkable ring signature）方案DualDory，且不需要任何信任机制。Hui等[28]发现了能够破坏DualDory[27]链接性的攻击，并提出改进方案LLRing-P以完善其安全性，二者具有相似的时空效率。以上2个LRS方案的签名大小和验证开销虽与环规模成对数关系，但其签名开销是线性的且包含较多耗时的双线性对运算，并且其验证过程依赖预计算，即仅在静态环时才能实现对数级的验证开销，以上特性限制了其在签名密集和动态环场景中的适用性。此外，Hui等[28]还提出了一个不依赖双线性对的LRS方案LLRing-DL，其验证开销是线性的，但面对小环时计算耗时更低。Xie等[29]设计的LRS方案通过引入基于双线性对的新型集合成员证明（SMA, set membership argument）实现了常量大小的签名，并且将验证过程的群幂运算和双线性对次数优化为常量（仅有限域乘法是线性的），但其签名过程仍包含线性的耗时运算。在目前的公开文献中，尚未见到在动态环时实现签名和验证开销同为常数级的环签名方案。可见，虽然环成员的信息必然以某种形式参与签名和验证过程（因此难以实现真正意义上的常数级计算开销），但将此线性部分完全置于轻量运算，进而使高耗时运算次数为常数，仍是实现常数级计算开销的有效途径。

可证安全性是公钥密码研究的重要部分。分叉引理由Pointcheval等[30]提出，已成为证明数字签名不可伪造性的核心工具。文献[31-33]在其基础上逐步扩展分叉引理的适用范围，依次建立了一般环签名、标识签名和标识环签名的形式化安全分析框架。特别地，赖建昌等[34]在RO模型下基于q-SDH假设严格证明了SM9数字签名算法满足自适应选择消息和身份攻击下的存在性不可伪造（EUF-CMIA, existential unforgeability under adaptive chosen-message-and-identity attack）安全性，为国密算法的安全应用提供了理论保障。

2 标识环签名概述

本节对符号含义、困难问题、系统模型和安全模型进行描述。

2.1 符号含义

表1列出了本文使用的主要符号及其含义，其余符号在首次出现时定义。

表1 主要符号及其含义

符号	含义
G_1, G_2	椭圆曲线加法循环群
G_T	乘法循环群
N	大素数，群G_1, G_2, G_T的阶
P_1, P_2	群G_1, G_2的生成元
Z_N^*	$[1, N-1]$范围内整数构成的群
Z_N	$[0, N-1]$范围内整数构成的群
λ	安全参数
params	系统公开参数
msk	签名主私钥
ID	用户身份标识
M	待签名消息
U	环成员集合$\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_n\}$
ds	用户签名私钥
$\boldsymbol{\sigma}$	环签名消息
ψ	同态映射：$G_2 \to G_1$
$x \in_R X$	从X（集合、群等）中随机选择元素x
negl(λ)	可忽略函数，输出随λ扩大而迅速趋零
$[k]V$	椭圆曲线点V的k倍（标量乘）
H_1, H_2	哈希函数：$\{0,1\}^* \to Z_N^*$
$x \| y$	x与y的字节串拼接
e	双线性对：$G_1 \times G_2 \to G_T$

为避免与公开参数P_1, P_2混淆，另以P, Q指代困难问题实例中群G_1, G_2的生成元。

2.2 困难问题

标识签名的安全性依赖q-SDH假设[34]。

定义1 q-SDH问题（q-strong Diffie-Hellman problem）。令秘密整数$a \in Z_N^*$，给定实例$(P, Q, [a]Q, [a^2]Q, \cdots, [a^q]Q) \in G_1 \times G_2^{q+1}$，且满足$[a^i]P = \psi([a^i]Q), i = 0,1,\cdots,q$，计算任意一组$\left(c, \left[\frac{1}{c+a}\right]P\right)$，其中$c \in Z_N$。

如果该问题在多项式时间的求解概率可忽略，则其困难假设成立。

2.3 系统模型

IBRS方案一般包含Setup、KeyGen、RingSign和RingVerify这4个算法[11]，其概要信息如表2所

表2　IBRS系统模型

算法名称	中文含义	执行者	算法性质	输入	输出
Setup	系统建立	KGC	PPT算法	λ	**params**, **msk**
KeyGen	用户签名私钥生成	KGC	确定性算法	**params**, ID, **msk**	ds
RingSign	环签名生成	签名者	PPT算法	**params**, M, U, ds	$\boldsymbol{\sigma}$
RingVerify	环签名验证	验证者	确定性算法	**params**, M, U, $\boldsymbol{\sigma}$	accept / reject

示。其中，KGC表示密钥生成中心，PPT表示概率多项式时间，签名者标识ID $\in U$，验证者可由知晓系统公开参数的任意实体担任，验证通过输出accept，否则输出reject。方案的运行流程如图1所示。

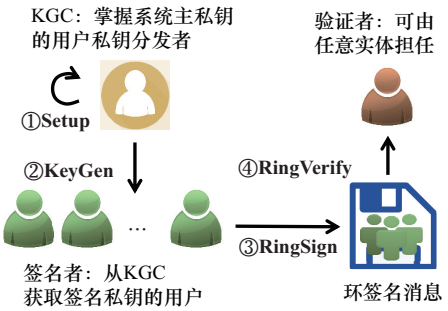


图1　方案运行流程

2.4　安全模型

IBRS方案必须实现2项安全性[35]：EUF-CMIA；匿名性。

定义2　EUF-CMIA。该性质由挑战者C与PPT敌手A的交互游戏定义。

1) 初始化。C生成(**params**, **msk**)并公开**params**。

2) 询问。A按需向C查询私钥或签名。

3) 伪造。A输出挑战用户集合U^*、消息M^*和环签名$\boldsymbol{\sigma}^*$（U^*中标识对应的私钥及U^*对M^*的签名均未被询问）。若$\boldsymbol{\sigma}^*$通过验证，则A获胜。

若A获胜的优势$\mathrm{Adv}_A^{\mathrm{EUF}} = \Pr[\mathrm{RingVerify}(\mathbf{params}, M^*, U^*, \boldsymbol{\sigma}^*) \to \mathrm{accept}] \leqslant \mathrm{negl}(\lambda)$，则称IBRS方案满足EUF-CMIA安全性。

定义3　匿名性。与定义2的游戏框架类似，步骤1)和步骤2)相同，区别如下。

3) 挑战。A指定挑战用户集合U^*、消息M^*和2个标识$\mathrm{ID}_1^*, \mathrm{ID}_2^* \in U^*$。$C$选择$b \in_R \{0,1\}$，以$\mathrm{ID}_b^*$的私钥生成$U^*$对$M^*$的签名$\boldsymbol{\sigma}^*$，并将$\boldsymbol{\sigma}^*$发送给$A$。

4) 猜测。A输出$b' \in \{0,1\}$。若$b'=b$，则A获胜。

若A获胜的优势$\mathrm{Adv}_A^{\mathrm{ANON}} = \Pr[b'=b] - \frac{1}{2} \leqslant \mathrm{negl}(\lambda)$，则称IBRS方案满足匿名性。

$$\Pr\left[\mathrm{RingVerify}(\mathbf{params}, M, U, \boldsymbol{\sigma}) \to \mathrm{accept} \,\middle|\, \begin{array}{c}\mathrm{Setup}(\lambda) \to (\mathbf{params}, \mathbf{msk}) \\ \mathrm{KeyGen}(\mathbf{params}, \mathrm{ID}, \mathbf{msk}) \to \mathrm{ds} \\ \mathrm{RingSign}(\mathbf{params}, M, U, \mathrm{ds}) \to \boldsymbol{\sigma}\end{array}\right] = 1 \tag{1}$$

$$\Pr\left[\mathrm{RingVerify}(\mathbf{params}, M, U, \boldsymbol{\sigma}') \to \mathrm{accept} \,\middle|\, \begin{array}{c}\mathrm{Setup}(\lambda) \to (\mathbf{params}, \mathbf{msk}) \\ \mathrm{FakeSign}(\mathbf{params}, M, U) \to \boldsymbol{\sigma}'\end{array}\right] \leqslant \mathrm{negl}(\lambda) \tag{2}$$

3　方案构造

本节对基于SM9的环签名方案的各个算法进行详细描述。

3.1　Setup

KGC选定一个1 B大小的签名私钥生成函数识别符hid，生成签名主私钥$\mathrm{ks} \in_R Z_N^*$，计算签名主公钥$P_{\mathrm{pub\text{-}s}} = [\mathrm{ks}]P_2 \in G_2$，公开$P_{\mathrm{pub\text{-}s}}$和hid。

3.2　KeyGen

设用户标识为ID，KGC计算$v = H_1(\mathrm{ID}\|\mathrm{hid}, N) \in Z_N^*$，$\mathrm{ds} = \left[\frac{\mathrm{ks}}{v+\mathrm{ks}}\right]P_1 \in G_1$，以秘密渠道向用户发送签名私钥ds。若$v+\mathrm{ks}=0$，则主密钥(ks, $P_{\mathrm{pub\text{-}s}}$)和全部用户的私钥均需更换。为简化表述，后文以$H_1(\mathrm{ID})$指代$H_1(\mathrm{ID}\|\mathrm{hid}, N)$。

3.3　RingSign

令签名者标识为$\mathrm{ID}_\pi \in U$（U中包含n个成员，$\pi \in \{1,2,\cdots,n\}$），其私钥记为ds_π。签名者预先计算$g_0 = e(P_1, P_{\mathrm{pub\text{-}s}}) \in G_T$，$g_1 = e(\mathrm{ds}_\pi, P_2) \in G_T$，$g_2 = e(\mathrm{ds}_\pi, P_{\mathrm{pub\text{-}s}}) \in G_T$，后续计算步骤如下。

1)$r, r_0 \in {}_{\mathrm{R}}Z_N^*$，$\omega = g_0^{\,r r_0} \in G_T$。

2)$v_i = H_1(\mathrm{ID}_i) \in Z_N^*$，$i = 1,\cdots,\pi-1,\pi+1,\cdots,n$。

3)r_1，r_2，…，$r_{\pi-1}$，$r_{\pi+1}$，…，r_n，$\rho \in {}_{\mathrm{R}}Z_N^*$，$\beta = \left(g_1^{\,r\sum_{i=1,i\neq\pi}^{n} r_i v_i} \cdot g_2^{\,r\sum_{i=1,i\neq\pi}^{n} r_i} \cdot g_0^{\,r\rho}\right)^{-1} \in G_T$。

4)$h = H_2(U\|M\|\omega\|\beta) \in Z_N^*$。

5)$r_\pi = \dfrac{r\,r_0 - h}{r} + \rho \in Z_N^*$，若$r_\pi = 0$，则返回步骤1)。

6)$S = [r]\mathrm{ds}_\pi \in G_1$。

7)输出环签名消息$\boldsymbol{\sigma} = (h, S, \beta, r_1, r_2, \cdots, r_n)$。

3.4 RingVerify

验证者预先计算$g_0 = e(P_1, P_{\text{pub-s}}) \in G_T$，收到$U'$对$M'$的环签名消息$\boldsymbol{\sigma}' = (h', S', \beta', r_1', r_2', \cdots, r_n')$后，验证步骤如下。

1) 检查$h', r_1', r_2', \cdots, r_n' \in Z_N^*$、$S' \in G_1$和$\beta' \in G_T$，若任一项不符合，则输出reject。

2) $v_i = H_1(\mathrm{ID}'_i) \in Z_N^*$，$i = 1, 2, \cdots, n$。

3)$\omega' = e\left(S', \left[\sum_{i=1}^{n} r_i' v_i\right] P_2 + \left[\sum_{i=1}^{n} r_i'\right] P_{\text{pub-s}}\right) \cdot g_0^{\,h'} \cdot \beta' \in G_T$。

4)$h'' = H_2(U'\|M'\|\omega'\|\beta') \in Z_N^*$。

5)若$h'' = h'$，输出accept，否则输出reject。

4 方案性质推导与证明

本节通过理论推导和安全规约，证明方案的正确性、不可伪造性和匿名性。

4.1 正确性

若签名与验证双方正确运行算法，且$U = U'$，$M = M'$，$\boldsymbol{\sigma} = \boldsymbol{\sigma}'$，$\omega'$推导如下。

$$\omega' = e\left(S', \left[\sum_{i=1}^{n} r_i' v_i\right] P_2 + \left[\sum_{i=1}^{n} r_i'\right] P_{\text{pub-s}}\right) \cdot g_0^{\,h'} \cdot \beta' =$$

$$e\left([r]\mathrm{ds}_\pi, \left[\sum_{i=1}^{n} r_i v_i\right] P_2 + \left[\sum_{i=1}^{n} r_i\right] P_{\text{pub-s}}\right) \cdot g_0^{\,h} \cdot \left(g_1^{\,r\sum_{i=1,i\neq\pi}^{n} r_i v_i} \cdot g_2^{\,r\sum_{i=1,i\neq\pi}^{n} r_i} \cdot g_0^{\,r\rho}\right)^{-1} =$$

$$e(\mathrm{ds}_\pi, P_2)^{\,r\sum_{i=1}^{n} r_i v_i} + e(\mathrm{ds}_\pi, P_{\text{pub-s}})^{\,r\sum_{i=1}^{n} r_i} \cdot g_0^{\,h-r\rho} \cdot e(\mathrm{ds}_\pi, P_2)^{-r\sum_{i=1,i\neq\pi}^{n} r_i v_i} \cdot e(\mathrm{ds}_\pi, P_{\text{pub-s}})^{-r\sum_{i=1,i\neq\pi}^{n} r_i} =$$

$$e(\mathrm{ds}_\pi, P_2)^{r r_\pi v_\pi} \cdot e(\mathrm{ds}_\pi, P_{\text{pub-s}})^{r r_\pi} \cdot g_0^{\,h-r\rho} =$$

$$e(\mathrm{ds}_\pi, [r r_\pi]([v_\pi] P_2 + P_{\text{pub-s}})) \cdot g_0^{\,h-r\rho} =$$

$$e\left(\left[\frac{\mathrm{ks}}{v_\pi + \mathrm{ks}}\right] P_1, \left[r\left(\frac{r r_0 - h}{r} + \rho\right)(v_\pi + \mathrm{ks})\right] P_2\right) \cdot g_0^{\,h-r\rho} =$$

$$e([\mathrm{ks}] P_1, [r r_0 - h + r\rho] P_2) \cdot g_0^{\,h-r\rho} =$$

$$g_0^{\,r r_0 - h + r\rho} \cdot g_0^{\,h-r\rho} = g_0^{\,r r_0} = \omega$$

故$h'' = H_2(U \| M \| \omega \| \beta) = h$。因此，本文方案满足正确性。

4.2 不可伪造性

本文方案的不可伪造性由EUF-CMIA模型定义。

定理1 若H_1, H_2为RO，且q-SDH问题是困难的，则本文方案在EUF-CMIA模型下是安全的。

证明 假设EUF-CMIA模型中的PPT敌手A获胜的优势ε不可忽略，则可构建模拟器B求解q-SDH问题。B接收q-SDH问题实例$(P, Q, [a]Q, [a^2]Q, \cdots, [a^q]Q)$后，与$A$的交互如下。

1) 初始化。B生成$q+1$个两两互异的整数$w^*, w_1, w_2, \cdots, w_q \in {}_{\mathrm{R}}Z_N^*$，令多项式$f(x) = \prod_{i=1}^{q}(w_i + x)$，由问题实例和$f(x)$计算$P_1 = [f(a)]P$，$P_2 = Q$，$P_{\text{pub-s}} = [a]Q$（$\mathrm{ks} = a$隐式存在），生成$i^* \in {}_{\mathrm{R}}\{1, 2, \cdots, q\}$，建立2个记录哈希询问的列表$L_1, L_2$。

2) 哈希询问。H_1和H_2是B掌握的RO，令非重复询问数分别为q_{H_1}, q_{H_2}，且$q_{H_1} = q$。A（或B自身）随时可发起询问，若L_1或L_2存在询问记录，则直接答复，否则B的处理方式如下。

① H_1询问。设第i次询问的输入为ID_i，答复$H_1(\mathrm{ID}_i) = \begin{cases} w^*, i = i^* \\ w_i, i \neq i^* \end{cases}$，将$(i, \mathrm{ID}_i, H_1(\mathrm{ID}_i))$记录至$L_1$。

② H_2询问。设第j次询问的输入为U_j、M_j以及$\omega_j, \beta_j \in G_T$，生成$h_j \in {}_{\mathrm{R}}Z_N^*$，答复$H_2(U_j \| M_j \| \omega_j \| \beta_j) = h_j$，将$(j, U_j, M_j, \omega_j, \beta_j, h_j)$记录至$L_2$。

3) 询问。该阶段A可按需向B进行以下询问。

① 私钥询问。设输入为ID_i，B查找L_1记录$(i, \mathrm{ID}_i, H_1(\mathrm{ID}_i))$（若无，先进行$H_1$询问）。若$i = i^*$，则中止；否则，$B$令多项式$f_i(x) = x\prod_{j=1, j\neq i}^{q}(w_j + x)$，由问题实例和$f_i(x)$计算其签名私钥$\mathrm{ds}_i = [f_i(a)]P = \left[\dfrac{a \cdot f(a)}{w_i + a}\right]P = \left[\dfrac{\mathrm{ks}}{H_1(\mathrm{ID}_i) + \mathrm{ks}}\right]P_1$并返回。

②签名询问。设输入为U和M，B选择$\mathrm{ID}_\pi \in {}_{\mathrm{R}}U$（$\pi \neq i^*$），利用私钥$\mathrm{ds}_\pi$计算环签名$\boldsymbol{\sigma}$并返回。

4) 伪造。A 输出挑战用户集合 $U^*=\{\mathrm{ID}_1^*,\mathrm{ID}_2^*,\cdots,\mathrm{ID}_n^*\}$、消息 M^* 和环签名 $\boldsymbol{\sigma}^*$（U^* 中标识对应的私钥及 U^* 对 M^* 的签名均未被询问）。若 $\mathrm{ID}_{i^*}\notin U^*$，则中止；否则，根据分叉引理，若 A 在未持有 U^* 中任一用户私钥时伪造了有效的 $\boldsymbol{\sigma}^*$，则 B 可构造图灵机 A'，在 A 的帮助下以同一输入 (M^*,U^*) 获取 2 个有效的环签名 $\boldsymbol{\sigma}_1^*=(h_1^*,S^*,\beta^*,r_1^*,\cdots,r_{\pi-1}^*,r_{\pi,1}^*,r_{\pi+1}^*,\cdots,r_n^*)$ 和 $\boldsymbol{\sigma}_2^*=(h_2^*,S^*,\beta^*,r_1^*,\cdots,r_{\pi-1}^*,r_{\pi,2}^*,r_{\pi+1}^*,\cdots,r_n^*)$，满足 $h_1^*\neq h_2^*,r_{\pi,1}^*\neq r_{\pi,2}^*$。若 $\mathrm{ID}_\pi^*\neq\mathrm{ID}_{i^*}$，则中止；否则，令 $\dfrac{x\cdot f(x)}{w^*+x}=F(x)+\dfrac{d}{w^*+x}$，多项式 $F(x)$ 的系数和非零整数 d 可由 w^* 和 $f(x)$ 计算。B 计算 $W^*=\left[\dfrac{1}{d}\right]\left(\left[\dfrac{r_{\pi,1}^*-r_{\pi,2}^*}{h_2^*-h_1^*}\right]S^*-[F(a)]P\right)$，输出 (w^*,W^*) 作为 q-SDH 问题实例的解。

由于 $r_{\pi,1}^*=\dfrac{r^*r_0^*-h_1^*}{r^*}+\rho$，$r_{\pi,2}^*=\dfrac{r^*r_0^*-h_2^*}{r^*}+\rho$，$S^*=[r^*]\,\mathrm{ds}_{i^*}=\left[\dfrac{r^*a}{w^*+a}\right]P_1=\left[\dfrac{r^*a\cdot f(a)}{w^*+a}\right]P$，则有

$$W^*=\left[\frac{1}{d}\right]\left(\left[\frac{r_{\pi,1}^*-r_{\pi,2}^*}{h_2^*-h_1^*}\right]S^*-[F(a)]P\right)=$$

$$\left[\frac{1}{d}\left(\frac{(r^*r_0^*-h_1^*)-(r^*r_0^*-h_2^*)}{r^*(h_2^*-h_1^*)}\cdot\frac{r^*a\cdot f(a)}{w^*+a}-F(a)\right)\right]P=$$

$$\left[\frac{1}{d}\left(\frac{a\cdot f(a)}{w^*+a}-F(a)\right)\right]P=$$

$$\left[\frac{1}{d}\left(F(a)+\frac{d}{w^*+a}-F(a)\right)\right]P=\left[\frac{1}{w^*+a}\right]P$$

故 (w^*,W^*) 是有效的解。

只有当 B 成功模拟、A 伪造私钥的标识恰好为 ID_{i^*}（概率为 $\dfrac{1}{q_{H_1}}$），且此时 A 伪造的签名有效（优势为 ε）时，B 才能成功求解 q-SDH 问题。由于其概率 $\dfrac{\varepsilon}{q_{H_1}}$ 不可忽略，与 q-SDH 假设相矛盾，故本文方案在 EUF-CMIA 模型下是安全的。证毕。

4.3　匿名性

本文方案具备完全匿名性，即使系统签名主私钥泄露或敌手具有无限计算能力，也无法辨别环签名消息的实际签名者。

定理 2　如果环签名生成时的随机数源符合均匀分布，则本文方案满足匿名性。

证明　设环签名 $\boldsymbol{\sigma}=(h,S,\beta,r_1,r_2,\cdots,r_n)$ 由 U 中用户生成。假设签名者为 ID_{π_1}（$\pi_1\in\{1,2,\cdots,n\}$），则 $r_{\pi_1}=\dfrac{r\,r_0-h}{r}+\rho$，$S=[r]\,\mathrm{ds}_{\pi_1}=\left[\dfrac{r\cdot\mathrm{ks}}{v_{\pi_1}+\mathrm{ks}}\right]P_1$

$$\beta=\left(g_1^{\,r\sum\limits_{i=1,i\neq\pi_1}^{n}r_iv_i}\cdot g_2^{\,r\sum\limits_{i=1,i\neq\pi_1}^{n}r_i}\cdot g_0^{\,r\rho}\right)^{-1}=$$

$$e(\mathrm{ds}_{\pi_1},[-r\sum_{i=1,i\neq\pi_1}^{n}r_i\,(v_i+\mathrm{ks})]\,P_2)\cdot g_0^{-r\rho}=$$

$$e\left([\mathrm{ks}]\,P_1,\left[\frac{-r\sum\limits_{i=1,i\neq\pi_1}^{n}r_i(v_i+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}-r\rho\right]P_2\right)$$

而签名者也可视为 ID_{π_2}（$\pi_2\in\{1,2,\cdots,n\}\setminus\{\pi_1\}$），这是因为，令 $r'=\dfrac{r(v_{\pi_2}+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}$，$\rho'=r_{\pi_2}+\dfrac{(v_{\pi_1}+\mathrm{ks})(h-r\,r_0)}{r(v_{\pi_2}+\mathrm{ks})}$，有 $r'\rho'=r'r_{\pi_2}+h-r\,r_0$，则

$$S=\left[\frac{r(v_{\pi_2}+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}\cdot\frac{\mathrm{ks}}{v_{\pi_2}+\mathrm{ks}}\right]P_1=[r']\,\mathrm{ds}_{\pi_2}$$

$$\beta=e\left([\mathrm{ks}]\,P_1,\left[\frac{-r(v_{\pi_2}+\mathrm{ks})\sum\limits_{i=1,i\neq\pi_2}^{n}r_i(v_i+\mathrm{ks})}{(v_{\pi_1}+\mathrm{ks})(v_{\pi_2}+\mathrm{ks})}+r\,r_{\pi_1}-\frac{r\,r_{\pi_2}(v_{\pi_2}+\mathrm{ks})}{v_{\pi_1}+\mathrm{ks}}-r\rho\right]P_2\right)=$$

$$e\left([\mathrm{ks}]\,P_1,\left[\frac{-r'\sum\limits_{i=1,i\neq\pi_2}^{n}r_i(v_i+\mathrm{ks})}{(v_{\pi_2}+\mathrm{ks})}+r\,r_0-h+r\rho-r'r_{\pi_2}-r\rho\right]P_2\right)=$$

$$e(\mathrm{ds}_{\pi_2},[-r'\sum_{i=1,i\neq\pi_2}^{n}r_i\,(v_i+\mathrm{ks})]\,P_2)\cdot g_0^{-r'\rho'}=\left(e(\mathrm{ds}_{\pi_2},P_2)^{\,r'\sum\limits_{i=1,i\neq\pi_2}^{n}r_iv_i}\cdot e(\mathrm{ds}_{\pi_2},P_{\mathrm{pub-s}})^{\,r'\sum\limits_{i=1,i\neq\pi_2}^{n}r_i}\cdot g_0^{\,r'\rho'}\right)^{-1}$$

又因为 $r_{\pi_2}=\dfrac{r'r_0'-h}{r'}+\rho'$，则 $r_0'=\dfrac{r'r_{\pi_2}+h-r'\rho'}{r'}=\dfrac{r_0(v_{\pi_1}+\mathrm{ks})}{v_{\pi_2}+\mathrm{ks}}$，且 $r'r_0'=r\,r_0$，即 $\boldsymbol{\sigma}$ 同样符合由 ID_{π_2} 作为签名者的计算过程推导。

当环签名过程采用的随机数源满足均匀分布时，签名者 ID_{π_1} 的随机数 $(r, r_0, r_1, \cdots, r_{\pi_1-1}, r_{\pi_1+1}, \cdots, r_n, \rho)$ 和签名者 ID_{π_2} 的随机数 $(r', r_0', r_1, \cdots, r_{\pi_2-1}, r_{\pi_2+1}, \cdots, r_n, \rho')$ 都是随机且独立的，即使在计算能力无限且掌握主私钥ks的敌手来看，判断 $\boldsymbol{\sigma}$ 的签名者是 ID_{π_1} 还是 ID_{π_2} 时仍无任何优势，故无法在集合 U 内辨认实际签名者。因此，本文方案满足完全匿名性。证毕。

5　性能分析与实验

本节在理论和实测层面，将本文方案的性能与同类方案[11-14]以及国际文献中的代表性方案[27-29]进行对比。

5.1　性能分析

首先量化各方案的计算开销和通信开销。表3列举了私钥生成、环签名生成和环签名验证这3个算法中各项耗时运算的次数。其中，SM_1, SM_2 分别表示群 G_1, G_2 上的标量乘，E表示群 G_T 上的幂，BP表示双线性对，n 表示环成员数量，—表示无上述耗时运算。有限域 F_N 上的运算、群 G_1, G_2 加法、群 G_T 乘法、哈希运算 H_1, H_2 等低耗时运算（合计占比不足2%）以及预计算步骤未计入分析结果。

本文方案的环签名生成与验证不需要像文献[11-12]方案对每个环成员逐项计算，也未引入文献[13-14]方案的密码累加器，而是通过相对轻量的有限域运算合并环成员信息，将各项耗时运算的次数降至常数级。此外，DualDory[27]和LLRing-P[28]的对数级验证开销是静态环开销，所需的预计算量分别为 $3n$BP 和 $3n\mathrm{BP}+n\mathrm{SM}_1$，二者在动态环时的验证开销仍是线性的。

对于通信开销，各方案系统公钥、用户私钥和环签名数据的长度如表4所示。其中，$|G_1|=33$ B、$|G_2|=65$ B、$|G_T|=384$ B、$|Z_N|=32$ B 表示对应群元素的比特数[9]，q 表示环成员的最大数量，N、P_1、P_2 等标准文件规定的公共参数未计入系统公钥。

表4　环签名方案的通信开销

方案	系统公钥	用户私钥	环签名数据
文献[11]	$\lvert G_2\rvert$	$\lvert G_1\rvert$	$n\lvert G_1\rvert+\lvert Z_N\rvert$
文献[12]	$\lvert G_2\rvert$	$\lvert G_1\rvert$	$\lvert G_1\rvert+(n+1)\lvert Z_N\rvert$
文献[13]	$2\lvert G_2\rvert+(q+4)\lvert G_1\rvert$	$\lvert G_1\rvert$	$2\lvert G_T\rvert+6\lvert G_1\rvert+8\lvert Z_N\rvert$
文献[14]	$2\lvert G_2\rvert+q\lvert G_1\rvert$	$\lvert G_1\rvert$	$\lvert G_2\rvert+2\lvert G_1\rvert+\lvert Z_N\rvert$
DualDory[27]	$q\lvert G_2\rvert+q\lvert G_1\rvert$	$\lvert Z_N\rvert$	$6\log n\lvert G_T\rvert+2\lvert G_2\rvert+7\lvert G_1\rvert$
LLRing-P[28]	$q\lvert G_2\rvert+q\lvert G_1\rvert$	$\lvert Z_N\rvert$	$(6\log n+10)\lvert G_T\rvert+11\lvert Z_N\rvert$
文献[29]	$q\lvert G_2\rvert+2q\lvert G_1\rvert$	$\lvert Z_N\rvert$	$5\lvert G_2\rvert+10\lvert G_1\rvert+\lvert Z_N\rvert$
本文方案	$\lvert G_2\rvert$	$\lvert G_1\rvert$	$\lvert G_T\rvert+\lvert G_1\rvert+(n+1)\lvert Z_N\rvert$

文献[11-12]方案及本文方案的公私钥与标准SM9数字签名算法一致。文献[13-14,29]方案以系统公钥与 q 线性相关为代价，实现常数级环签名长度；文献[27-28]方案的环签名长度为对数级；其余方案的环签名长度与 n 线性相关；本文方案的环签

表3　环签名方案的计算开销

方案	私钥生成	环签名生成	环签名验证
文献[11]	SM_1	$(n+1)\mathrm{SM}_1+(n-1)\mathrm{SM}_2+(n-1)\mathrm{E}+n\mathrm{BP}$	$n\mathrm{SM}_2+n\mathrm{E}+n\mathrm{BP}$
文献[12]	SM_1	$\mathrm{SM}_1+(3n-2)\mathrm{E}$	$3n\mathrm{E}+2\mathrm{BP}$
文献[13]	SM_1	$(2n+13)\mathrm{SM}_1+4\mathrm{E}+2\mathrm{BP}$	$(n+13)\mathrm{SM}_1+5\mathrm{E}+5\mathrm{BP}$
文献[14]	SM_1	$(2n+4)\mathrm{SM}_1+\mathrm{SM}_2+\mathrm{E}+\mathrm{BP}$	$(n+1)\mathrm{SM}_1+\mathrm{E}+3\mathrm{BP}$
DualDory[27]	SM_1	$3n\mathrm{SM}_1+2n\mathrm{SM}_2+10n\mathrm{BP}$	$10\log n\ \mathrm{E}$
LLRing-P[28]	SM_1	$2n\mathrm{SM}_1+2n\mathrm{SM}_2+10n\mathrm{BP}$	$10\log n\ \mathrm{E}$
文献[29]	—	$(4n+12)\mathrm{SM}_1+2n\mathrm{SM}_2$	$5\mathrm{SM}_1+7\mathrm{SM}_2+17\mathrm{BP}$
本文方案	SM_1	$\mathrm{SM}_1+4\mathrm{E}$	$2\mathrm{SM}_2+\mathrm{E}+\mathrm{BP}$

名数据相较文献[12]增加1个群G_T元素。

5.2　实验测试

基于Python国密算法库hggm[36]实现各方案并进行对比测试。实验计算机配置如表5所示。

表5　　实验计算机配置

项目	配置
设备类型	PC
操作系统	Windows10 64位
CPU	Intel Core i3-10110U（2核心4线程）
内存	8 GB LPDDR3 2 133 MHz
硬盘	SAMSUNG MZVLB512HBJQ-000L7
Python版本	3.7.1

设环成员数量n为4、16、64、256、1 024，各方案环签名生成与验证耗时如表6所示（单位为ms，每项实验中表现最佳和次佳的数据分别加粗和加下划线），本文方案相较文献[12,14,29]方案的计算性能加速比如图2所示。结果为500次测试均值，不含预计算开销。

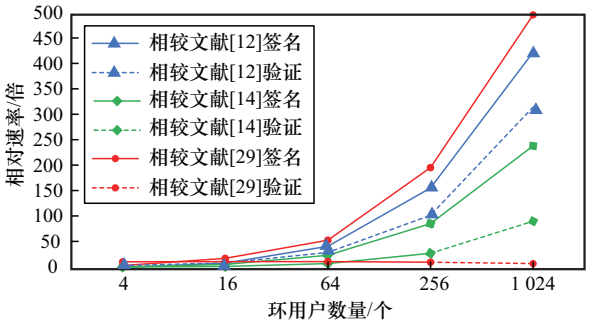


图2　本文方案相较其他方案的计算性能加速比

由表4和表6可知，当n由4增至1 024时，本文方案签名与验证、文献[29]方案验证的耗时涨幅较小，近似地实现了常数级开销，文献[27-28]方案的验证耗时呈对数级增长，而其他方案/算法的耗时均随n线性增长。当n = 1 024时，相较本实验中的次佳方案（文献[14]签名和文献[29]验证），本文方案的签名与验证效率分别为其241.61倍和10.11倍；即使计入通信开销（文献[14,29]方案及本文方案需传递的环签名长度分别为163 B、687 B和33 217 B），在100 Mbit/s带宽下，本文方案综合效率分别为二者的226.15倍和9.61倍；在1 Mbit/s带宽下，本文

表6　　各个算法测试结果

方案	算法	环成员数量/个				
		4	16	64	256	1 024
文献[11]	环签名生成	120.64	518.89	2081.45	8 318.94	33.79×10^3
文献[12]		<u>48.29</u>	227.20	940.43	3 844.81	15.79×10^3
文献[13]		114.26	215.55	602.45	2 179.59	9 027.81
文献[14]		71.12	<u>171.43</u>	<u>563.53</u>	<u>2 143.69</u>	<u>8 954.21</u>
DualDory[27]		1 074.79	4 246.11	16.97×10^3	71.42×10^3	280.71×10^3
LLRing-P[28]		1 050.32	4 119.80	16.72×10^3	67.42×10^3	278.32×10^3
文献[29]		121.53	413.12	1 188.39	4 819.38	18.52×10^3
本文方案		**19.70**	**20.65**	**21.35**	**24.21**	**37.06**
文献[11]	环签名验证	123.38	510.07	2 042.32	8 168.26	33.46×10^3
文献[12]		202.64	377.50	1 081.27	3 895.66	15.46×10^3
文献[13]		199.33	246.44	440.29	1 230.05	4 655.11
文献[14]		<u>101.52</u>	<u>149.82</u>	<u>343.99</u>	1 134.24	4 546.05
DualDory[27]		241.18	490.18	739.27	993.78	1 257.53
LLRing-P[28]		234.44	486.63	726.14	985.96	1 234.00
文献[29]		457.46	468.56	477.89	<u>482.35</u>	<u>491.48</u>
本文方案		**33.38**	**33.17**	**33.83**	**37.17**	**48.59**

方案综合效率仍为二者的30.83倍和1.64倍。进一步地（仍令$n = 1\ 024$），本文方案的签名效率具有比较优势的最低带宽为6.76 kbit/s，验证效率具有比较优势的最低带宽为79.25 kbit/s。即除少数低带宽场景（如低功耗蓝牙）外，本文方案的综合开销仍优于常数级签名长度的方案。

综上，本文方案将环签名生成与验证开销降至常数级，较现有方案显著提升了计算效率，尤其在较大环规模时优势突出。

6 结束语

本文提出基于国密算法SM9的高效环签名方案，核心创新在于通过优化群运算结构，将签名和验证过程中涉及环规模的线性运算转移至轻量级的有限域，使耗时运算（包括椭圆曲线标量乘、群G_T上的幂和双线性对）次数降为常数，而现有方案至少有一项耗时运算是线性的。在保持不可伪造性和完全匿名性可证安全的前提下，本文方案实现了计算性能上的突破：即使考虑通信开销，其综合效率仍显著高于环签名定长的最优对比方案。本文方案的不足之处在于环签名长度仍是线性的，不利于环规模较大时的通信和存储，下一步将研究完全常数级的环签名方案。

参考文献：

[1] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//2001 International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Berlin: Springer, 2001: 552-565.

[2] LI X F, MEI Y R, GONG J, et al. A blockchain privacy protection scheme based on ring signature[J]. IEEE Access, 2020, 8: 76765-76772.

[3] 饶金涛, 崔喆. 基于SM9盲签名与环签名的安全电子选举协议[J]. 计算机工程, 2023, 49(6): 13-23, 33.
RAO J T, CUI Z. Secure e-voting protocol based on SM9 blind signature and ring signature[J]. Computer Engineering, 2023, 49(6): 13-23, 33.

[4] SUN S F, AU M H, LIU J K, et al. RingCT 2.0: a compact accumulator-based (linkable ring signature) protocol for blockchain cryptocurrency monero[C]//2017 European Symposium on Research in Computer Security (ESORICS). Berlin: Springer, 2017: 456-474.

[5] 薛婧婷, 刘亮, 李发根, 等. 双边隐私保护的能源交易多方计算方案[J]. 密码学报, 2025, 12(1): 96-116.
XUE J T, LIU L, LI F G, et al. Dual-side privacy-preserving multi-party computation for energy trading[J]. Journal of Cryptologic Research, 2025, 12(1): 96-116.

[6] ABE M, OHKUBO M, SUZUKI K. 1-out-of-n signatures from a variety of keys[C]//Advances in Cryptology-ASIACRYPT 2002. Berlin: Springer, 2002: 415-432.

[7] ZHANG F G, KIM K. ID-based blind signature and ring signature from pairings[C]//Advances in Cryptology-ASIACRYPT 2002. Berlin: Springer, 2002: 533-547.

[8] KANG J N, WEN F T. A linkable ring signature scheme on lattice from DualRing[C]//Proceedings of the 2024 6th International Conference on Electronics and Communication, Network and Computer Technology (ECNCT). Piscataway: IEEE Press, 2024: 426-430.

[9] 国家市场监督管理总局 国家标准化管理委员会. 信息安全技术 SM9标识密码算法 第1部分：总则: GB/T 38635.1—2020[S]. 北京: 中国标准出版社, 2020.
Standardization Administration of the People's Republic of China. Information security technology—Identity-based cryptographic algorithms SM9: Part 1: General: GB/T 38635.1—2020[S]. Beijing: Standards Press of China, 2020.

[10] 国家市场监督管理总局 国家标准化管理委员会. 信息安全技术 SM9标识密码算法 第2部分：算法: GB/T 38635.2—2020[S]. 北京: 中国标准出版社, 2020.
Standardization Administration of the People's Republic of China. Information security technology—Identity-based cryptographic algorithms SM9: Part 2: Algorithms: GB/T 38635.2—2020[S]. Beijing: Standards Press of China, 2020.

[11] 彭聪, 何德彪, 罗敏, 等. 基于SM9标识密码算法的环签名方案[J]. 密码学报, 2021, 8(4): 724-734.
PENG C, HE D B, LUO M, et al. An identity-based ring signature scheme for SM9 algorithm[J]. Journal of Cryptologic Research, 2021, 8(4): 724-734.

[12] 谢振杰, 张耀, 杨启超, 等. 基于国密算法SM9的环签名方案[J]. 计算机科学, 2025, 52(12): 384-390.
XIE Z J, ZHANG Y, YANG Q C, et al. A ring signature scheme based on domestic cryptographic algorithm SM9[J]. Computer Science, 2025, 52(12): 384-390.

[13] 安浩杨, 何德彪, 包子健, 等. 基于SM9数字签名的环签名及其在区块链隐私保护中的应用[J]. 计算机研究与发展, 2023, 60(11): 2545-2554.
AN H Y, HE D B, BAO Z J, et al. Ring signature based on the SM9 digital signature and its application in blockchain privacy protection[J]. Journal of Computer Research and Development, 2023, 60(11): 2545-2554.

[14] 谢振杰, 尹小康, 蔡瑞杰, 等. 基于国密算法SM9的可追踪环签名方案[J]. 通信学报, 2025, 46(3): 199-211.
XIE Z J, YIN X K, CAI R J, et al. Traceable ring signature scheme based on domestic cryptographic algorithm SM9[J]. Journal on Communications, 2025, 46(3): 199-211.

[15] 蒲浪, 林超, 伍玮, 等. 基于国密SM9的公钥认证可搜索加密方案[J]. 软件学报, 2025, 36(9): 4271-4284.
PU L, LIN C, WU W, et al. Public-key authenticated encryption scheme with keyword search from Chinese cryptographic SM9[J]. Journal of Software, 2025, 36(9): 4271-4284.

[16] 周权, 陈民辉, 卫凯俊, 等. 基于SM9的支持策略隐藏的可追踪属性签名[J]. 计算机研究与发展, 2025, 62(4): 1065-1074.
ZHOU Q, CHEN M H, WEI K J, et al. Traceable attribute-based signature for SM9-based support policy hidden[J]. Journal of Computer Research and Development, 2025, 62(4): 1065-1074.

[17] 刘行, 明洋, 王晨豪, 等. 基于SM9的可验证公平标识广播代理重加密[J]. 计算机学报, 2025, 48(3): 721-737.
LIU H, MING Y, WANG C H, et al. Verifiable and fair identity-based broadcast proxy re-encryption based on SM9[J]. Chinese Journal of Computers, 2025, 48(3): 721-737.

[18] LIU X H, HUANG X Y, CHENG Z H, et al. Fault-tolerant identity-

based encryption from SM9[J]. Science China Information Sciences, 2024, 67(2): 104-117.

[19] LIN C Y, WU T C. An identity-based ring signature scheme from bilinear pairings[C]//Proceedings of the 18th International Conference on Advanced Information Networking and Applications - Volume 2. New York: ACM Press, 2004: 182-185.

[20] HERRANZ J, SÁEZ G. New identity-based ring signature schemes[C]// Information and Communications Security. Berlin: Springer, 2004: 27-39.

[21] CHOW S S M, YIU S M, HUI L C K. Efficient identity based ring signature[C]//Applied Cryptography and Network Security. Berlin: Springer, 2005: 499-512.

[22] BRAKERSKI Z, KALAI Y T. A framework for efficient signatures, ring signatures and identity based encryption in the standard model[J]. IACR Cryptology ePrint Archive, 2010(86): 1-45.

[23] DODIS Y, KIAYIAS A, NICOLOSI A, et al. Anonymous identification in ad hoc groups[C]//Advances in Cryptology - EUROCRYPT 2004. Berlin: Springer, 2004: 609-626.

[24] NGUYEN L. Accumulators from bilinear pairings and applications[C]// Topics in Cryptology-CT-RSA 2005. Berlin: Springer, 2005: 275-292.

[25] HU C Y, LIU P T. An enhanced constant-size identity-based ring signature scheme[C]//Proceedings of the 2009 2nd IEEE International Conference on Computer Science and Information Technology. Piscataway: IEEE Press, 2009: 587-590.

[26] 邓浩明, 彭长根, 丁红发, 等. 基于国密SM9算法的门限环签名方案[J]. 计算机技术与发展, 2022, 32(12): 95-102.
DENG H M, PENG C G, DING H F, et al. A threshold ring signature scheme based on GM SM9 algorithm[J]. Computer Technology and Development, 2022, 32(12): 95-102.

[27] BOOTLE J, ELKHIYAOUI K, HESSE J, et al. DualDory: logarithmic-verifier linkable ring signatures through preprocessing[C]//Computer Security – ESORICS 2022. Berlin: Springer, 2022: 427-446.

[28] HUI X Y, CHAU S C. LLRing: logarithmic linkable ring signatures with transparent setup[C]//Computer Security – ESORICS 2024. Berlin: Springer, 2024: 299-319.

[29] XIE M, TU Z Z, AU M H, et al. Efficient constant-size linkable ring signatures for ad-hoc rings via pairing-based set membership arguments[C]//Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2025: 858-872.

[30] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[31] HERRANZ J, SÁEZ G. Forking lemmas for ring signature schemes[C]// Progress in Cryptology - INDOCRYPT 2003. Berlin: Springer, 2003: 266-279.

[32] 周瑾, 张亚娟, 祝跃飞. 一般的基于身份签名体制与Forking引理[J]. 信息工程大学学报, 2007, 8(2): 129-133.
ZHOU J, ZHANG Y J, ZHU Y F. Generic ID-based signature schemes and forking lemma[J]. Journal of Information Engineering University, 2007, 8(2): 129-133.

[33] 周敏, 傅贵, 周权. 分叉引理对一般基于身份环签名体制的证明[J]. 通信技术, 2008, 41(7): 183-184, 188.
ZHOU M, FU G, ZHOU Q. Proof of generic ID-based ring signature by forking lemma[J]. Communications Technology, 2008, 41(7): 183-184, 188.

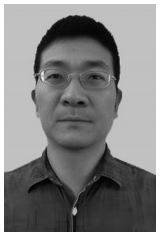
[34] 赖建昌, 黄欣沂, 何德彪, 等. 国密SM9数字签名和密钥封装算法的安全性分析[J]. 中国科学: 信息科学, 2021, 51(11): 1900-1913.
LAI J C, HUANG X Y, HE D B, et al. Security analysis of SM9 digital signature and key encapsulation[J]. Scientia Sinica (Informationis), 2021, 51(11): 1900-1913.

[35] BENDER A, KATZ J, MORSELLI R. Ring signatures: stronger definitions, and constructions without random oracles[J]. Journal of Cryptology, 2009, 22(1): 114-138.

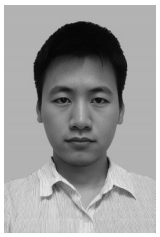
[36] 谢振杰, 刘奕明, 蔡瑞杰, 等. 国密算法SM9的性能优化方法[J]. 计算机科学, 2025, 52(6): 390-396.
XIE Z J, LIU Y M, CAI R J, et al. Performance optimization method for domestic cryptographic algorithm SM9[J]. Computer Science, 2025, 52(6): 390-396.

[作者简介]

谢振杰（1995– ），男，湖南湘潭人，信息工程大学博士生，主要研究方向为云安全、密码学应用。

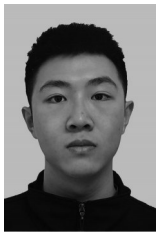


刘胜利（1973– ），男，河南周口人，博士，信息工程大学教授、博士生导师，主要研究方向为网络设备安全、网络攻击检测。



贾志鹏（2001– ），男，辽宁兴城人，信息工程大学博士生，主要研究方向为物联网设备安全、二进制代码分析。

翟锦源（2004– ），男，河南周口人，信息工程大学助理工程师，主要研究方向为网络空间安全。



刘成（2004– ），男，安徽六安人，信息工程大学硕士生，主要研究方向为网络空间安全。